Review of
.uk Registration Policy

Lord Macdonald QC

December 2013

Summary of Recommendations

- Nominet should remain an open registry. Amongst other reasons set out in the body of this Review, this is because the market in domain names requires a speedy and efficient registration process and because the screening technology currently available is blunt and incapable of judging context. In circumstances where Nominet registers between 150,000-200,000 new domain names every month, this inevitably means that any pre-registration scrutiny of applications will throw up unmanageable numbers of false positives, slowing down registrations to no purpose and to a point that is likely to become commercially unviable.

- Nominet should consider instituting a system of post-registration screening, to be conducted within 48 hours of registration, for domain names that appear to signal sex crime content, or to amount in themselves to sex crimes. Where examples in this category are discovered, they should be reported to the police and suspended or de-registered. This process, in so far as it is designed to detect grave criminality, is plainly consistent with an open registration policy.

- Nominet should restrict post registration scrutiny to domain names in the serious sex crime category. This is because the relevant screening terms for sex crime are highly specific and have a stronger chance of identifying true positives. Post-registration screening for other forms of criminality will inevitably rely on very general terms that are bound to throw up unmanageable numbers of false positives.

- Nominet, which is a private company, should have no role in policing questions of taste or offensiveness on the Internet. It is not set up, trained or by culture competent to act as Internet censor, in contrast to identifying possible examples of criminality for onward reporting to the police. Furthermore, there are no objective, generally accepted standards of taste that could guide Nominet in undertaking such a role. This means that any decision-making on its part would risk uncertainty and inconsistency, which are highly undesirable ingredients where the restriction of free expression rights is concerned. Nominet would not have public confidence as censor, and it should not be expected to assume such a role in circumstances where government and police are content not to act.

- Where domain names that are alleged to signal criminal content, or to amount to crimes in themselves, or to be attached to criminal content, are brought to Nominet's attention, Nominet should, if it agrees that they might fall into any of those categories, refer these cases to the police for further action. In consultation with the police, this could include suspension or de-registration. It is only in these circumstances that Nominet, which is not a content provider, should involve itself in the examination of website content for any regulatory purpose.

- Nominet should amend its terms and conditions to make it clear that any registration of a domain name that signals criminal content, or amounts in itself to a crime, will constitute a breach of Nominet's terms of business, and is liable to be reported to the police and suspended or de-registered.

1. INTRODUCTION

1.1 The .uk country code Top Level Domain ('ccTLD') came into existence in July 1985 and was initially operated on an informal basis by volunteers from the UK Internet community. Domain name registrations were allocated by a "Naming Committee" free of charge on a quasi-manual basis. By the mid 1990s, this position became unsustainable and after some debate and consultation, Nominet was incorporated as private company limited by guarantee for the purpose of administrating the .uk ccTLD.

1.2 Since 1996 Nominet has administered the registry database and name server infrastructure, which enables domain names to be used for web browsing and email. In practice Nominet does not deal directly with the registrants of domain names, leaving this to its network of registrars who have automated access to the Nominet registration systems.

1.3 Nominet has around 3,000 registrars which include almost all UK Internet Service Providers ('ISPs'), as well as media organisations such as the BBC and other parties who prefer to manage their own domain names. Registrars typically provide other services such as web hosting and design, and email provision in addition to domain name registration.

1.4 Almost without exception, Nominet's registrars are also members of Nominet, which enables them to vote for directors of the company. Being a member of Nominet results in a much lower cost for registration of domain names; £3.50 for one year, £5.00 for two years.

Domain name market dynamics

1.5 Nominet has been very successful. There are now over 10.5 million .uk domain names (the vast majority being co.uk) which makes .uk the third largest ccTLD in terms of number of domain names under management, and the fifth largest domain registry worldwide after taking into account .com and .net domains. The latest Domain Name Industry Brief published by VeriSign the US for-profit company, which administers the .com and .net domains, is attached at *Appendix 1*. Nominet's share of domain names registered in the UK is around 50% with its main competitor being .com (see new registrations market share, *Appendix 2*).

Current domain registration rules

1.6 The registration process is now formalised and governed by Rules (see *Appendix 3*) and Terms and Conditions (*see Appendix 4*), which explain the registration process and obligations on Nominet and its registrants.

1.7 Nominet's Terms and Conditions currently provide that identity and contact information provided must be accurate, and that registration and use of a domain name must not infringe third party intellectual property rights (7.3 and 7.4 of the Terms and Conditions). However, although breach of the Terms and Conditions may result in suspension or deregistration, the obligations placed on domain name registrants are, apparently intentionally, minimal and do not include conditions forbidding the use of obscene words or phrases.

1.8 This is because Nominet operates an open registration system. This means that electronic applications for a domain name are accepted, without vetting, on a 'first come, first served' basis, and that there are no restrictions as to who may register co.uk and org.uk domains (*Rule 4.4*). The fact that registrants do not need to be UK domiciled is seen as an indicator of .uk's credibility in a competitive international market, as well as an important manifestation of the UK government's declared support for an open Internet.

1.9 The only restrictions applicable to domain names administered by Nominet are set out in *Rule 5*, namely that:

- a domain name must consist only of the characters a-z, 0-9 and hyphens
- the first and last characters of a domain name must not be a hyphen
- domain names must not start with "xn- -" (this is used in some registrations systems for non-latin scripts and accented characters etc)
- at the third level, the second levels used within .uk (co, org, ac, etc) are reserved for policy reasons, together with "com" and "uk"
- the total length of a domain name may not be more than 64 characters in total

1.10 It will therefore be apparent that Nominet has intentionally taken a non-restrictive approach to the words and phrases that may be used in a domain name. Nominet has historically not made any value judgements as to the use to which domains are put, or whether they might be offensive or in poor taste. This has also been the practice adopted by other open registries such as .com, .eu and .org, and in many other ccTLDs.

1.11 Some ccTLDs, such as .ie (Republic of Ireland) have naming policies which state that a domain name must not be offensive or contrary to public policy or generally accepted principles of morality.

1.12 Rightly or wrongly, the philosophy behind Nominet's approach has been based upon the notion that, absent demonstrated abuse at an extreme level, the Internet should offer access that is as free as possible to the widest number of

people, including to people whose taste and judgment are seriously open to question.

1.13 On this analysis, the .uk domain space is not intended to be, and can never amount to, an indicator of British moral values, in so far as there is in any event a national consensus around questions of taste or decency (which I doubt), except in so far as those values espouse freedom of expression and consequent open relations around the world. Different considerations may apply to domain names blatantly signalling or inciting very serious crime, as I explain later in this Review, since it is possible that these amount to crimes in themselves.

Current restrictions on the use of domain names

1.14 However, in apparent recognition of the open nature of the registration system, and commercial abuses that might thereby result, Nominet does provide a dispute resolution service (DRS), which allows complaints to be brought relatively quickly and cheaply against registrations that appear to be taking unfair advantage of third party rights. Around 60 complaints are made via an online form each month, typically on the basis of trademark infringement. Compared with between 150,000 – 200,000 new domain registrations made each month this appears to be an effective and proportionate countermeasure to abuse of the open first come, first served allocation policy. Similar Alternative Dispute Resolution ('ADR') processes exist for almost all other TLDs.

1.15 For more serious issues such as criminal use, Nominet has apparently established working relationships with law enforcement agencies such as the National Crime Agency, the Metropolitan Police's e-Crime Unit and Trading Standards, under which an expedited suspension process (that is to say removing the functionality of a domain name whilst maintaining it on the database of registrations) is successfully used.

1.16 In relation to child sexual abuse material, Nominet is a member of the Internet Watch Foundation ('IWF'), the Internet industry funded charitable organisation that issues take down notices and maintains a blocking list in relation to child sexual abuse material and extreme pornography online. Nominet is thereby bound to follow any requests for any removal action that IWF may request. Typically, these would be in relation to child sexual abuse material, since IWF rarely seeks to take action against adult pornography, except in its most extreme forms.

1.17 In practice, Nominet deals with only a handful of law enforcement suspension requests each month (mostly for counterfeit goods and prescription

medicines) and has never, in fact, received a request or complaint from the IWF. In recent years, no .uk site has been found to host child sexual abuse content, probably because the UK has a well-earned reputation as a hostile environment for such material.

Some recent concerns

1.18 In August 2013, an article was published in the *Sunday Times* expressing concern about the volume of Internet adult pornography hosted in Britain, and in particular about the lack of restrictions on pornographers registering domain names with Nominet.

1.19 It was suggested in this article, and later endorsed by some parliamentarians, experts and campaigners, that the open registration system operated by Nominet effectively created a situation in which any .uk domain name not previously registered was available for registration. This meant that any domain name, however offensive or crude in its phrasing, and even if it appeared to glorify serious crime, could be obtained from Nominet by the simple expedient of visiting its website, selecting the desired domain name and paying the fee.

1.20 This open system, it was argued, provided insufficient protection against the registration of wholly unacceptable domain names on .uk. The only real obligation was to provide a registrant name, along with address details, which Nominet's registration process recognised as being likely to constitute a real, rather than an invented address. So long as an applicant passed this very basic test, he or she could obtain whichever domain name had been selected.

1.21 As a result of the expression of these concerns, the Nominet Board decided to review its policy on registrations. In particular, the Board wished my Review to consider whether Nominet should maintain its open registration policy, or move instead to a system of pre-registration screening of applications for .uk domain names, in order that it might weed out those deemed to be in some way 'unacceptable'.

1.22 Further, the Board wished consideration to be given to the extent to which, if at all, Nominet should become involved in policing the content of .uk sites, so that it should, again, take action against those thought to be 'unacceptable'. Finally, the Board wished to receive an assessment of Nominet's treatment of complaints from the public relating to .uk domain names on the grounds of taste, decency or pornographic or other apparently criminal content.

2. THE CONSULTATION

2.1 I have been greatly assisted by a careful consideration of the many responses to the public consultation undertaken by Nominet in connection with my Review. This consultation took the form of an invitation published on the Nominet website to members of the public to send in their comments on a range of issues connected to Nominet's business, its open registration policy and possible reforms to that policy. A summary of responses via the Nominet website is to be found at *Appendix 5.*

2.2 I also met, as a part of this public consultation, with a wide range of police and civilian experts, parliamentarians, departmental officials, NGO representatives, registrars, campaigners and other interested parties. A full list of those I have spoken to in connection with my Review is to be found at *Appendix 6.*

2.3 I think it fair to say that, broadly speaking, the majority of respondents to the consultation were cautious about Nominet's moving away from an open registration policy and adopting a more regulatory approach to the registration of domain names. Such support as there was for a system of screening against applications was generally predicated upon the notion that this was not a matter of applying criteria of taste or decency to those applications, which would be vague and subjective and, in the view of this category of respondent, gravely undermining of an open Internet, but rather of developing a process that might reliably weed out domain names thought to be in some way 'criminal'.

2.4 There was, however, a strong scepticism regularly expressed by the majority of respondents, particularly amongst those who claimed specialist knowledge in this area, that technology is presently equipped accurately to screen words and terms with the precision that would be necessary were such a process of pre-registration screening to be effective, even in the case of the most extreme words and terms.

2.5 I have, of course, borne in mind that many responses to a consultation of this sort will emanate from those who have some specialist, industry or even ideological interest in the outcome of any Review. This is not to minimise the importance of such responses, but simply to situate them accurately. A consultation is not an opinion poll.

2.6 In any case, there were also contrary views from those who expressed strong support for a greater degree of pre-registration scrutiny designed to block the registration of domain names containing certain words or phrases, or

apparently signalling particular content, including in the case of both domain names and content words and terms that were insulting, crude or offensive.

2.7 These responses supported the view that Nominet, as the UK's 'virtual flagship', has a duty to scrutinise in advance applications for .uk domain names, in order to refuse applications for names that are, for one reason or another, deemed to be inappropriate for inclusion in the .uk space.

3. THE LEGISLATIVE AND POLICY FRAMEWORK

3.1 *Article 8* of the *European Convention on Human Rights ('ECHR')* states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

3.2 *Article 10* of the *European Convention of Human Rights* states:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

3.3 It will readily be seen that under the ECHR, neither privacy rights nor free expression rights are absolute and each may be restricted in certain circumstances, so long as any such restrictions are proportionate, prescribed by law, and necessary in a democratic society for a permitted purpose.

3.4 No doubt it is partly because of its strong attachment to ECHR privacy and free expression rights, that the UK government is equally strongly attached to the principle of an open Internet that is as far a possible self-, rather than state, regulated. As Ed Vaizey, the minister responsible for the government Internet policy, said in his speech to the Nominet Policy Forum in 2012:

> *[W]e have policy goals that we would like to achieve, but we're not dogmatic or rigid in how we go about achieving those policy goals. ... So, we don't mandate solutions to them, in fact we want self-regulatory*

solutions,.... But overriding all of that is our absolute commitment to an open internet'.

'[O]ur over-riding aim should be to protect the essential openness of the net. ... Self-regulation should clearly be our first option here'

'The speed at which new innovations spring up and usage changes is partly why the multi-stakeholder approach to governance is important and why regulation and the heavy-hand of Government is not well placed to deliver the safety and security Internet users depend on'.

3.5 In his speech to the Nominet Policy Forum in 2011, Mr Vaizey said:

'So the question for me is how we make the most of the open internet, maintaining it as an engine for growth and innovation, whilst safeguarding people's data and protecting them and their children from harmful or inappropriate activities and content online.

'Let me be clear, I don't think regulation is the answer here – a lightly regulated Internet is good for business, good for the economy. Frankly, it's good for all of us.'

3.6 Similarly, Ed Richards, the Chief Executive of Ofcom said in a speech on Internet and consumer protection that he gave on 11 October 2012:

'Let me also say a few words about web blocking – an area that I know is of great concern to many of you.

'We all recognise how the Internet has enabled a revolution in innovation, democracy and public debate, and we have seen increased public scrutiny, transparency and accountability as a result.

'We do not want this to change. We are mindful of the threat there would be to innovation online if open Internet access was compromised'.

3.7 In this context, it is notable that the European Court of Human Rights has repeatedly made clear that Article 10 protects not only speech which is well-received and popular, but also speech which is offensive, shocking or disturbing (*Sunday Times v UK (No2)*[1992]14EHRR123):

"*Freedom of expression constitutes one of the essential foundations of a democratic society ... it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also as to those that offend, shock or disturb".*

3.8 The English common law takes a similar approach. In *Chambers v DPP* [2012] EWHC 2157 (Admin), the Lord Chief Justice made it clear that:

"*Satirical, or iconoclastic, or rude comment, the expression of unpopular or unfashionable opinion about serious or trivial matters, banter or humour, even if distasteful to some or painful to those subjected to it should and no doubt will continue at their customary level, quite undiminished by [section 127 of the Communications Act 2003].*"

3.9 Sedley LJ reminded the courts in *Redmond-Bate v DPP [2000] H.R.L.R. 249* that:

"*free speech includes not only the inoffensive but the irritating, the contentious, the eccentric, the heretical, the unwelcome and the provocative provided it does not tend to provoke violence. Freedom only to speak inoffensively is not worth having*".

3.10 The Court noted that, as argued in *Hammond*, a "*heckler's veto",* would not only offend the European Convention, but the English common law as well.

3.11 In most circumstances, the Court concluded,

"*the burden normally falls upon the viewer to avert further bombardment of [his] sensibilities by simply averting his eyes"*. After all, the "*purpose of all speech protection...is to shield just those choices of content that in someone's eyes are misguided, or even hurtful*".

3.12 In a case regarding the banning of an electoral broadcast by the Pro- Life Alliance, Lord Scott said:

"Indeed, in my opinion, the public in a mature democracy are not entitled to be offended by the broadcasting of such a programme. A refusal to transmit such a programme based upon the belief that the programme would be "offensive to very large numbers of viewers" (the letter of 17 May 2001) would not, in my opinion, be capable of being described as "necessary in a democratic society ... for the protection of ... rights of others". Such a refusal would, on the contrary, be positively inimical to the values of a democratic society, to which values it must be assumed that the public adhere"

3.13 Finally, in a recent decision concerning potential tort liability for the intentional infliction of emotional distress by disgraceful and abusive Wetsboro Baptist Church protests at the funerals of dead American servicemen, the United States Supreme Court was concerned that a jury is

"*unlikely to be neutral with respect to the content of (such) speech,*

posing a real danger of (their) becoming an instrument for the suppression of ...vehement, caustic and sometimes unpleasant expression". [such a risk was] "*unacceptable: in public debate [we] must tolerate insulting, and even outrageous speech in order to provide adequate breathing space for the freedoms protected by the first amendment".*

3.14 To summarise, the freedom to receive and impart ideas and information may not be absolute under European jurisprudence, but any restrictions must be proportionate and necessary in a democratic society. Exceptions to the right to free expression must be narrowly interpreted and their necessity convincingly and strictly established.

3.15 We live in a world in which electronic communication and the Internet are central to life, to commerce, and to human progress. In those circumstances, the maintenance of the highest degree of protection for free expression rights in those arenas would appear to be critical and a public good in its own right. An Internet free from unnecessary restriction is a boon not just to the human spirit, and to that spirit's essential ingredients: the right to speak, write and broadcast freely, but also to the development of trade, commerce, knowledge and invention.

3.16 As I have already indicated, it is no doubt for these reasons that the UK government is, as a matter of declared policy, very strongly supportive of a free and open Internet. Such a position is also consistent with the UK's long history of respect for fundamental rights, including the right to free expression, the open exchange of ideas, free trade and comity between nations.

3.17 Furthermore, this stance would not appear to be in any way inconsistent with recent government initiatives that have successfully led to Google and Microsoft announcing the blocking of certain search terms that appear to relate to seriously illegal content, mainly sexual in nature. Unlike Nominet, of course, these companies directly provide content platforms, so that blocking technology may clearly be appropriate in their cases where serious criminality is suspected or may be in prospect.

4. A REGULATORY ROLE FOR NOMINET?

4.1 It is, I believe, within the context of repeated court judgments in the UK, Europe and the USA, stressing the importance of free expression rights and the extent to which those rights encompass the right to insult and to offend, that the desirability of Nominet's developing a broader policy of regulation in relation to domain names must be assessed. I say 'broader', because it is sensible to start by acknowledging that Nominet already appears to accept that it has some role in regulating not just domain names, but even the content of .uk websites as well.

4.2 For example, Nominet has terms of business and presumably reserves the right to suspend or to de-register domain names registered in breach of its terms and conditions. It also operates a Dispute Resolution Service ('DRS') that deals, amongst other things, with complaints that websites registered to .uk are guilty of, for example, trademark infringement. These are referred, under the DRS, to a panel of expert arbitrators engaged by Nominet to make adjudications, by which the parties agree to be bound. Suspension or de-registration of a domain name may take place after such a process.

4.3 I also understand that Nominet has developed good working arrangements with law enforcement agencies so that in the case of .uk websites that apparently offer counterfeit goods or fake medicines, Nominet will refer them to the police and, in appropriate cases, suspend or de-register a domain name on this basis in consultation with police.

4.4 As I have previously indicated, Nominet is a also member of IWF and will therefore refer apparent child sexual abuse material to that body, and also accept recommendations from IWF to remove offending material from the .uk space by suspending or de-registering a domain name.

4.5 It is, however, critical to note that the examples I have cited are all instances of action being taken *post-registration*, and relate either to commercial disputes brought to Nominet's attention by interested parties, or to action resulting from cases of apparent criminality fit to be referred to the police.

4.6 Very importantly, they also represent action taken after an examination of website *content,* rather than as a result of the consideration of a domain name alone.

4.7 Furthermore, in neither example does a decision to suspend or de-register a domain name result from an assessment of the facts made by Nominet itself. In the case of commercial disputes, an expert arbitrator makes a judgment of

the facts as part of the DRS process. In the case of apparent criminality, it is the police who make an assessment of the law. Thus it is only after those apparently equipped to do so have made their judgements, that Nominet will act to suspend or to de-register a domain name.

4.8 No doubt what underlies Nominet's reluctance to act of its own initiative in such circumstances, is its judgement, right or wrong, that it is not best equipped to make adjudications relating to commercial disagreements, still less to make judgements about criminality, particularly in the context of website content.

Some possible extensions to Nominet's regulatory role

4.9 But the question that arises in the context of this Review is whether Nominet should, in fact, be more proactive in regulating the nature of domain names. Should it act to weed out categories of domain name of its own initiative, without necessarily involving the police, or any other state agency, so that it assumes an important new role as Internet *censor*? Should it take upon itself a new role as regulator of .uk website *content,* as well as .uk domain names, which appear to represent the present limit of its responsibility?

4.10 To answer these questions, it is helpful to consider possible categories of domain names that might be the preferred target of such scrutiny. This is not straightforward, but it seems to me that they may conveniently be set out in three separate groups. These are those domain names that appear on their face to:

- Signal illegal content
- Incite criminal offences, so that they may amount to crimes in themselves
- Contain insulting, offensive or obscene words or phrases

4.11 In other words, in the first category might fall domain names that appear to indicate the presence on a website of extreme pornography, so that a seeker after such material might be attracted to the site by what is, in effect, an explicit invitation. An example might be www.bestialityhere.co.uk.

4.12 In the second category might fall domain names that on their face, and without any apparent need to examine further any content, appear to amount to criminal incitements. An example might be www.killredheads.co.uk if such a site could be taken seriously.

4.13 In the third category might fall all those domain names using crude or obscene terms, such that the name itself is sufficiently offensive to warrant rejection by

Nominet. Examples are too numerous and too obvious to set out here, although on one analysis they could include a well known and long standing media campaign conducted by a famous British fashion chain: FCUK.

4.14 There are, I think, difficulties with each of these categories. That does not necessarily lead to a clear conclusion that no action should or could be taken against any particularly 'bad' examples of any of them, as I explain later in this Review. But is does appear to mean that any censoring action against them would need to be very carefully targeted and within the narrowest of parameters, if grossly inappropriate interference in free speech rights, and corresponding damage to the whole concept of an open Internet are to be avoided. Again, I return to this later.

(i) *Signalling illegal content*

4.15 Alleged 'signalling' as a marker for the blocking, suspension or de-registration of certain domain names, appears to be a concept with some very problematic features. It is not unknown, for example, for domain names to be ironic, or deliberately misleading in respect of content, in order to create shock or for simple comic effect. Inappropriate action against domain names in this category would be a very serious interference in free expression rights and highly undermining of an open Internet, in contrast to the UK government's strong support of such an institution in the wider British national interest.

4.16 In addition, the whole notion of a domain name as an advert for the content of a website is highly controversial, with the Advertising Standards Authority, amongst others, disputing the usefulness of the concept. Many domain names, of course, never have any content attached to them at all. Indeed at the point of registration and for some time afterwards, all domain names are likely to be freestanding and quite lacking in any contextualising content to set against the alleged signalling.

4.17 Finally, for reasons which I set out later, pre-registration screening for domain names in this *entire* category is likely to be so cumbersome and inexact a process as to be wholly impracticable. As I argue later, this may not exclude post-registration scrutiny in *particular* categories.

(ii) *Inciting crime*

4.18 So far as the second category is concerned, 'incitement' is a complex legal concept, the utility of which would not appear readily to transfer to the terms of a domain name. In particular, to sustain an allegation of incitement under the criminal law, it is necessary to prove, as a basic element of the offence, that

the suspect intended the crime allegedly incited actually to take place. This would, I think, be highly problematic in the case of a domain name, except in the most extreme examples.

4.19 Of course, it might be possible to create a definition of incitement for these purposes that applied more readily to the use of particular words or phrases in domain names. But this would, I think, be an unhappy solution. Even to demonstrate, to the degree necessary to justify an act of censorship, that an individual wished, by the terms of a domain name, to 'encourage' a crime would likely prove extremely difficult in the context of evidence of such 'encouragement' residing simply in a domain name and nowhere else.

4.20 This is not, however, to deny that some domain names may be capable of amounting to crimes in themselves. However, since almost all domain names have no content attached to them at the point of registration, or indeed for some time afterwards, and many never have any content attached to them, any contextualising material to support an adverse conclusion will usually be absent. This means, as I argue later, that such examples would have to be in most egregious category safely to merit regulatory action.

4.21 Finally, for reasons that I set out later, pre-registration screenings for domain names in this *entire* category are likely to be so cumbersome and inexact a process as to be wholly impracticable.

(iii) *The use of offensive or obscene words*

4.22 As far as the third category is concerned, it may be sufficient to observe that it is fatally broad, so that determinations in this area would necessarily be highly subjective and, in the unavoidable absence of any reliable or generally accepted objective standard, markedly inconsistent. Subjective judgments on the part of a private company like Nominet on questions of taste and decency, leading to inconsistent decision-making around Internet censorship, would hardly be acceptable where they are bound to amount to gross interferences in free expression rights.

4.23 I also have little doubt that censorship on these grounds and by these means would also amount to a breach of Articles 8 and 10 of the European Convention. This is because it would plainly offend against the principle that free speech rights, in particular, include the right to express offensive and even shocking speech, and because it would frequently lead to restrictions in expression that are obviously not 'prescribed by law'. As one very obvious example, it is not illegal to swear.

4.24 It is, perhaps, useful to note in this context that, in 2012, the government removed the term 'insulting' from section 5 of the Public Order Act, so that the use of insulting words in a public place is no longer unlawful per se. This was in response to Parliament's strongly expressed concern that the criminalisation of the use of 'insulting words' in public was seriously undermining of free speech principles.

4.25 For these reasons, I do not believe it would be desirable or appropriate for Nominet to become involved in making judgments about taste or decency in the context of domain names, either before or after registration. Even were such judgments to be called for in the context of an open internet, there is no reason to suppose that Nominet has the skills that would be required to make those judgments and there is no reason at all to believe that the government would wish to take over such a role for itself. Indeed, it rightly refuses categorically to do so, since this would be to place very significant restrictions upon the Internet quite inconsistent with the broad thrust of government policy.

4.26 Furthermore, it seems to me highly unlikely that a private organisation like Nominet would attract any degree of public confidence in exercising a censoring role based upon its own inclinations, in circumstances where is it clear that the UK government is disinclined, as a matter of policy, to act, still less to legislate.

4.27 I understand the government's perfectly rational view to be that if something is lawful off the Internet, it should be equally lawful online. The converse, of course, is equally true, but it is worth noting that the government's stance allows for a very great deal that is grossly offensive on the Internet, without any fear of regulatory, still less law enforcement response.

4.28 It appears that it would be quite wrong for a private organisation like Nominet, in the absence of any proper authority, to manoeuvre itself into this breach and to initiate a private process of restriction of core Convention rights by inserting its own judgements into a space that the government and the police prefer not to occupy.

4.29 For these reasons, and because it is in no sense a content provider, I consider that it would be particularly undesirable for Nominet to assume any role whatsoever in censoring Internet *content.* It is plainly not equipped for such a task and it could not therefore be in the public interest for it to assume this role, particularly in the clear absence of any government or law enforcement desire to take up this highly sensitive function.

5. WHAT IS TECHNOLOGICALLY POSSIBLE?

5.1 But there is another important question, to which I have already alluded, beyond those raised by conflicting views as to what may be *desirable* in terms of pre-registration scrutiny. This further question is: what is actually technologically *possible*? How targeted is the technological scrutiny currently available, and what is it reasonably capable of achieving?

5.2 Nominet registers between 150,000– 200,000 .uk domain names every month. It is certainly true that it would be possible to screen all applications, in advance of approval, against a list of terms and phrases in order to signal, for example, domain names that include obscene words or terms.

5.3 The difficulty is, however, that screening technology of this sort is incapable of assessing context in any way. This is particularly so where the screening is being directed towards a domain name rather than to any content on a website, which is the process in prospect. In these circumstances, any screening is bound to result in vast numbers of false positives.

5.4 This is because, as I explain in Chapter 7 of this Review, indicator terms such as 'rape' may occur in a multitude of entirely innocent contexts. For example, many domain names containing the word 'rape' may offer counselling or advice services, or refer to agricultural seed. Equally, the word may be picked up in a term like 'therapist'. A well-known Internet pen retailing company called Pen Island notoriously boasts the domain name www.penisland.net. This appears to be inadvertent. And a screen for a particular Anglo Saxon term will falsely identify any phrase containing the letters that make it up, for example, Scunthorpe.

5.5 These are not trivial examples. Rather, they point to very real difficulties inherent in any attempt to match a multitude of screening terms against hundreds of thousands of registrations every month. The result, in the case of an extensively maintained list of forbidden terms and phrases, is bound to be a quite unmanageable number of false positives, requiring time-consuming examination by analysts, hardly suited to the purpose, to avoid the commercial and rights-offending disaster of repeatedly rejecting or delaying registrations that are, in fact, entirely appropriate in the first place.

5.6 It is very instructive to note that during 2013, Nominet conducted an operation in which it screened .uk domain names against a long list of terms and phrases maintained by the Internet Watch Foundation ('IWF'), for the purposes of IWF's work in identifying for blocking and removing child sexual abuse material from the internet. This process of scrutiny resulted in tens of thousands of positives, each of which was forwarded for examination to IWF.

5.7 Their analysts' conclusion was each 'positive' that they examined was false and no example of child sexual abuse material was identified from this operation. There is every reason to believe that this apparently pointless and, indeed, resource-hungry result would be endlessly replicated were per-registration screening against a broad range of terms to be adopted as a general policy.

5.8 It seems clear, therefore, that any process of pre-registration scrutiny is likely to be slow, technologically blunt, and have minimal useful impact. It would likely damage the credibility of the .uk space in the market place and it would bring few discernible advantages.

5.9 I understand that pre-registration scrutiny of this sort is not supported by IWF, because the experts in that highly regarded body take the clear view that such a process would be inefficient and incompetent in identifying problematic material. It would tie up time and resource to no great effect.

6. SOME CONCLUSIONS ON OPEN REGISTRATION

6.1 There appears to be a substantial risk that blanket pre-registration scrutiny would amount to a serious and disproportionate interference in the open Internet which, occurring in the context of the .uk domain space, would likely be very damaging to the UK's reputation for openness and the free passage of information and ideas. It would also be inefficient.

6.2 I therefore conclude that the maintenance of a list of 'undesirable' terms, against which registrations for .uk domain names should be screened in advance, would be unattractive for a number of reasons.

6.3 Firstly, it would slow down the registration process in a market place in which consumers expect, and can obtain, speed and certainty, to the detriment of the .uk space and therefore the national interest.

6.4 Secondly, the creation of a list of forbidden terms shorn of context is very likely indeed to result in anomalies and grave injustices and in a resulting chaotic assessment process. In particular, it would require Nominet staff to take on a role of Internet regulation in particularly sensitive areas for which they frankly seem to be ill equipped.

6.5 Thirdly, the involvement of Nominet, a private company, in making judgments about criminality in domain names, would appear to be highly problematic on its own terms. It is not clear what expertise Nominet would bring to such a task. This is equally pertinent to any suggestion that Nominet should set itself up as some sort of censor of Internet content. I have seen no evidence to suggest that the company is set up, or suited by culture, remit or training, to make important, finely balanced judgments requiring a degree of legal reasoning and necessarily impacting upon those critical free expression rights to which the UK is, by treaty and by longstanding inclination, so strongly attached.

6.6 In these circumstances, I conclude that Nominet's current policy of maintaining an open registration approach to the UK's virtual flagship is justifiable. This policy appears to accord appropriate respect to ECHR privacy and free expression rights and to the UK government's strong policy support for an open Internet, and it also reflects what is technologically possible within the context of an efficient and highly competitive ccTLD marketplace operating in a globalised world.

7. POST-REGISTRATION SCRUTINY

7.1 If it seems reasonably clear that pre-registration scrutiny is neither desirable nor practical, does the same apply to post registration scrutiny? In other words, should Nominet develop a process by which means it might satisfy itself, so far as it is technologically possible to do so within a scheme that is practical to operate, that no domain names that are beyond any reasonable standard of acceptability, are being registered in the .uk space?

7.2 For the purposes of this Review, I take it as read that some domain names may come into this category. It is likely that these could include domain names that appear clearly to signal paedophile content, or content relating to other serious sex crimes such as rape or bestiality, or amount to some form of incitement to commit those crimes.

7.3 It will be noted that these are all likely to be domain names that contain words or terms that either relate to acts that are patently contrary to criminal law or, alternatively, may amount to crimes in themselves, through the agency of incitement. Self evidently, they may be targeted without fear of any ECHR breach. It also seems likely that the presence of this category of sexual crime material on the Internet, as well as being plainly capable of removal in a manner entirely consistent with Convention rights, equally excites the deepest and strongest public disapproval.

7.4 Of course, a focus on this category of particularly grave criminality, that is to say serious sex crime, will not turn up other domain names that appear to signal or amount to crime more generally. But it is precisely because of the inadequacies of the screening technology that Nominet has available to it, and the utmost importance of avoiding unnecessary or mistaken interference with free expression rights, that any post registration screening process should be strictly designed to target only the most egregious examples, and those that may be most readily and efficiently picked up.

7.5 To expand on this point, it may be useful to consider the example of race hatred. In order to identify any 'inappropriate' domain names in this area, a term that might reasonably be screened for is 'kill'. But Nominet figures, which I discuss below, show that any attempt to screen for the term 'kill' in domain names returns quite unmanageable numbers of positives.

7.6 While this is hardly surprising, it does indicate the difficulty inherent in relying upon the identification of what are, in themselves, inoffensive words to identify unacceptable *combinations* of terms that might indicate race hate. This is particularly so where that unacceptability rests precisely upon context—

that is to say upon the relationship of those everyday words to other, equally unexceptional words, making up a domain name. An example here might be 'www.killblackpeople.co.uk'.

7.7 At my request, Nominet conducted a search for .uk domain names containing the word 'kill' and certain racial epithets.

7.8 The results showed that 10,379 .uk domain names contain the term 'kill'. Some examples include:

0-1waspkiller.co.uk
123skills.co.uk
24hourstokill.co.uk
50waystokillyourlover.co.uk
abcpresentationskills.co.uk
academyofmultiskills.co.uk
adultskillslearning.org.uk
aimtokill.co.uk

7.9 There are some 1,477 domains starting with the term kill, including:

kill-a-pest.co.uk
kill-a-vampire.co.uk
kill-bed-bugs.co.uk
killapool.co.uk
killaprints.co.uk
killar.co.uk
killerdeals.co.uk
kill-4-fun.co.uk

7.10 There are 14 domain names containing the sequential letters that make up the grossly offensive term 'nigger'. Five of these are in the formulation 'snigger'. Many of the 14 have no content, several appear to be attached to sites operated by commercial entities, or to 'comedy' sites of frankly dubious taste. Only one exhibits content, beyond the domain name itself, that appears to be grossly racially and sexually offensive, though it seems very unlikely indeed to be illegal in itself.

7.11 There are 547 domains containing the term 'paki.' None of these appear to be in any way offensive, still less illegal. Some examples include:

ampakistancatering.co.uk
apnapakistan.org.uk

book2pakistan.co.uk
call-pakistan.co.uk
clapakidz.org.uk

7.12 My conclusion from this survey is that post registration screening for terms that indicate some form of race hatred in a .uk domain name is unlikely to be fruitful in detecting illegality. This is because, given the bluntness in the technology that I have referred to earlier in this Review, potentially criminal domain names in this non-sexual category are likely to be impossible to pick up without the creation of so many false positives that the task becomes entirely chaotic and self-defeating. This will obviously apply to domain names referencing other categories of criminality outside sexual crime, too.

7.13 This is not, of course, to argue that domain names that are potentially criminal for reasons outside a sexual crime context, for example because they appear to incite racial hatred, should not attract regulatory attention. On the contrary, where they are identified and brought to Nominet's notice, any potentially criminal domain name in whatever category of crime should certainly be dealt with in the ways that I set out in Chapter 9 of this Review.

7.14 In other words, Nominet should refer any such domain names to the police and they should be subject, in consultation with the police, to suspension or de-registration. In this situation, any question of criminal prosecution arising would necessarily and properly be one for the police, not Nominet.

7.15 But it does appear to mean that Nominet should consider focussing any post-registration screening effort on potentially criminal sexual content, since this is more likely to introduce a mechanism that is both efficient and effective, at the same time as targeting domain names that are most likely to signal illegal content or amount to crimes in themselves.

7.16 It therefore seems to me that a deeper consideration of this issue should take into account five factors:

- Public disquiet at the most egregious examples of domain names that appear to breach any reasonable bounds of acceptability
- An acknowledgment that domain names in this category are almost always sexual and/or sexually criminal in nature
- The bluntness of the existing technology, which is incapable of assessing context, making it very difficult to screen for broader criminality
- The critical importance of free expression rights and the UK's stated support for an open internet
- Nominet's lack of competency as censor of Internet content

7.17 I think it arguable that, balancing these five factors, Nominet should consider acknowledging some role in protecting the .uk space from particularly stark examples of domain names that appears clearly to signal serious sex crime content, or to amount in themselves to serious sex crime. An important question, of course, is: would this work?

7.18 In August 2013, Nominet drew up a list of words describing a range of serious sex crimes. These words included 'paedophilia', 'bestiality', 'zoophilia', 'necrophilia' and so on. All new registrations were then screened against this list, within 24 hours of their registration. Nominet found that it was receiving around 20-25 positives each week against this list, the vast majority of which were false.

7.19 At the same time, Nominet screened these terms across its entire registry. It found that there are currently approximately 5832 active domains across the registry that have matches to the relevant list of words or their derivatives:

Term	**Current registrations**
%rape%	3145
%rapist%	2622
%incest%	55
%bestial%	1
%zoophil%	1
%necrophil%	1
%pedophil%/ %paedophil%	7
Total	5832

Table 1: Registration statistics

7.20 In the course of this exercise, Nominet found that:

- On average, 20.94 new registrations are made each week containing these terms or derivatives of these terms.
- Of 1089 such domains registered in the last year, 826 started with 'grape', 'drape', 'scrape' or 'princest' or contain 'therapist', 'draper', 'therapeutic' or 'rapeseed'.
- By way of example, 570 registrations containing a derivative of the term %rape% or %rapist% were registered in 2013 to date. 115 of these contain the term 'drape', 160 the term 'grape' and 105 the term 'therapeutic' accounting for two thirds of registrations with these terms.
- An initial scan of the domains with these terms indicated that 22 of these domains might warrant further inspection, but may not be problematic at

all, for example rape-of-the-working-class, which seems very likely to be political in nature.

'Innocent' registrations

7.21 It is, however, extremely important to note that these surveys confirmed that terms like 'incest' and 'rape' are contained in many more innocent domain names than in domains likely to be used for illegal purposes. For example, registrations may be for help or support lines for victims. There were, it transpired, a number of registrations for support and protest groups that contained the word 'paedophilia'.

7.22 It is equally the case that on very many occasions when the sequence of letters making up these terms appear, they do so in an entirely innocent context:

Term	**Example registrations**		
Rape	alisondraper.co.uk	ladrape.co.uk	bristolrapecrisis.org.uk
	bridge-parapets.co.uk	barbaraperkins.co.uk	
	rapecrisis.co.uk	rapeaware.co.uk	
Incest	princestrust.co.uk	vincestephens.co.uk	princestone.co.uk
	incestcounselling.org.uk		
paedophilia	paedophilia-research.org.uk		

Table 2: Example innocent registrations

'Bad registrations'

7.23 However, in the course of this work, Nominet also identified a number of examples of 'bad' domain names using terms or derivatives as outlined above. It categorised a 'bad' domain name as one whose terms indicated that it might be used for displaying imagery of illegal sexual acts. These examples, which are set out below in Table 3, were identified by using judgments based upon the name alone.

Term	**Domain name**
rape/rapist	rapeme.co.uk
	rapeporn.co.uk
	raper.co.uk
	asianrape.co.uk
	blackrape.co.uk
	arserape.co.uk
	rape.co.uk

	rapemyteacher.co.uk
	rapeslut.co.uk
	pornrape.co.uk
incest	incest.co.uk
	incesterotica.co.uk
	incestporn.co.uk
Bestial/bestiality	bestiality.co.uk
Zoophilia	zoophilia.co.uk
Necrophilia	necrophilia.co.uk
Paedophilia	paedophile.co.uk
	paedophiles.co.uk
	pedophile.co.uk

Table 3: Example 'bad' registrations

7.24 On the face of it, it is difficult to argue with the contention that at least some (but not all) of the 'bad' domain names set out in Table 3 above are examples of .uk domain names that Nominet might consider itself uncomfortable to host in the .uk space, even in the context of an otherwise open registration policy.

7.25 The basis of such reluctance in those cases would not, in my view, undermine in any way Nominet's attachment to open registration. It would simply be to acknowledge that it is difficult to see any reasonable basis whatsoever upon which the registration of a domain name such as rapemyteacher.co.uk could be consistent with any reasonable terms of business that Nominet might draw up.

7.26 Indeed, a screening of the sort I have described, taking place in the twenty four hours after registration, and targeting, in the manner of Nominet's test in August 2013, those domain names most likely to offend Nominet's terms and conditions, that is to say domain names likely to signal sexual crime content or likely to amount to sexual crime in themselves, would be entirely consistent with Nominet's remaining an open registry boasting a profound attachment to free expression rights.

7.27 It seems clear that the suspension or de-registration of domain names in this category would be equally consistent with the terms of Articles 8 and 10 of the ECHR. Examples of domain names in this category are likely to be very rare. But where they are discovered, it is easily arguable that their suspension or de-registration is a proportionate and necessary act in a democratic society, relating to material 'prescribed by law', that is to say, the portrayal or encouragement of serious sex crime, in order to protect vulnerable people and public morals.

7.28 It also appears very likely, from the results that I have set out, that such a process would be entirely manageable. Further, since the whole purpose of the exercise is to throw up the very worst cases, any difficulties inherent in identifying names likely to be in breach of Nominet's terms and conditions are likely to be minimised. It should be relatively straightforward for Nominet to set up a reliable in-house screening process to deal with these cases when they are picked up through the sort of post-registration screening that I have described.

7.29 It will be clear that this process would likely involve Nominet taking action in the absence of it having any opportunity to examine content attached to the apparently actionable domain name, since typically there will be none in the immediate period following registration. However I do not regard this as a disadvantage for two reasons.

7.30 Firstly, I think it unlikely that Nominet is equipped to make legal judgments about content, except in the most obvious cases, such as serious child sexual abuse material, which would be referred by Nominet to IWF in any event.

7.31 Secondly, the fact that no content is available to contextualise the domain name in any way is likely to result in only those names most patently and crudely inconsistent with Nominet's terms and conditions being actioned. In terms of avoiding unjustifiable interference in free expression rights and maintaining so far as possible an impeccably open Internet, this would amount to strength in the system.

7.32 Of course, if Nominet were to adopt this procedure, it would be necessary to mandate scrutiny of apparently non-compliant names at an appropriate level of seniority. It would also be necessary for Nominet to publish guidance for its staff to ensure, so far as possible, consistency in decision making.

7.33 Finally, great care would have to be taken to maintain a list of terms that was very strictly limited and defined to target the very worst examples, in order that the system might remain effective and manageable. It would be essential to avoid the sort of mission creep that might seriously threaten privacy and free expression rights on an Internet whose open character is so strongly advocated for by the UK government. For the avoidance of doubt, I repeat my view that questions of taste are no part of an appropriate remit for Nominet.

Nominet's terms and conditions

7.34 It would also be necessary, I think, for Nominet to give consideration to amending its terms and conditions to make it clear that registering a domain

whose name appears patently to signal serous sex crime content, or to amount to a serious sex crime on its own terms, amounts to a breach of its terms of business which may result in a report to the police and consequent suspension or de-registration.

8. A MORE TRANSPARENT REGISTER

8.1 During the course of the consultation, it has been suggested to me that Nominet might increase public confidence in the integrity and safety of the .uk space were it to make widely available for public examination the data base of all .uk registrations.

8.2 In the case of gTLDs like .com, .org and .net, zone file information relating to registered domain names is already made available to a wide range of authorised persons and entities, including law enforcement. This will also be the position for new domains, including .wales, .scot and .london, when they become available for registration next year.

8.3 The question arises as to whether a similar, more transparent policy should be followed by Nominet, since on one view this might have the effect of introducing a degree of policing by daylight tending to reduce the amount of 'unacceptable' material in the .uk space.

8.4 In this sense a more open register might help to reassure the public that Nominet's processes are adequate and functioning in an appropriate manner and are capable of rendering the .uk space as safe as possible, consistent with an open Internet and free expression rights, by empowering those who wish to challenge .uk registrations, on the grounds of 'acceptability' to do so. Self evidently, it is argued, this would increase public confidence to Nominet's benefit.

Zone files

8.5 Zone files contain the information needed to resolve domain names to Internet Protocol (IP) numbers. They contain domain names, their associated name server names and the IP addresses for those name servers. This means that a zone file lists all the active domain names within a particular zone.

The current picture

8.6 gTLDs are run under the ICANN umbrella and ICANN's stance is that gTLD zone file data should be available. An indicator of the rationale behind this view is the intended target audience for zone file data, which ICANN describes as:

- Internet Scholars & Researchers
- Intellectual Property Experts
- Security Experts
- Law Enforcement Professionals

8.7 gTLD zone file data is made available according to the terms of an ICANN template agreement. Under the current framework, this results in a series of bi-lateral agreements between zone file consumers and those individual gTLD registry operators who provide the data.

8.8 These bi-lateral access agreements provide for access to the zone file data under contractual terms, which require the party seeking access to accept limitations to how they will use the data. Chief amongst these limitations is that the data must not copied, shared, or further processed, except for certain proscribed reasons, and the data must not under any circumstances be used to support any sort of marketing activities.

8.9 In general, Internet users may be able to access and download zone file data at no cost for certain purposes. To do so, the Internet user must sign an agreement with the registry that operates that TLD. Approved users can access zone file data for at least three months, and download the zone file once per 24-hour period. Under certain circumstances, a Registry Operator may deny or revoke access.

The future

8.10 The Internet Corporation for Assigned Names and Numbers ('ICANN') is the private sector, non-profit corporation created in 1998 to assume responsibility for IP address spaces. ICANN seems committed to zone file publication as a principle and the Registry Agreement for the new gTLDs due to come online next year requires the operating registries to offer zone file access. The 2010 ICANN strategy paper dealing with this area of policy noted that:

> *'[S]everal stakeholder groups including anti-abuse and trademark protection organizations have described access to zone data as an effective and necessary tool for combating Domain Name System (DNS) abuse.'*

8.11 Clearly the expansion of the number of gTLDs will create an environment with considerably more gTLDs and gTLD operators and consequently ICANN has identified the need to find a model for managed zone file access that can be scaled up. Its 2010 strategy paper (see Appendix 7) envisaged a process designed to meet this challenge based on:

- A standardised relationship between zone file consumers and zone file providers.

- A clearing-house to manage the zone file access application process and credential checking of applicants so that consumers need only apply once regardless of the number of zone files they wish to access.

8.12 The framework within the gTLD namespace therefore allows for:

- Controlled access to zone file data by contract for approved users with verified credentials.
- Zone file data to be used for specified purposes only, mainly academic research, rights protection, or law enforcement.
- New procedures under development to ensure a unified approach to zone file data access following the introduction of new gTLDs next year.

ccTLD zone file access

8.13 CENTR is a not-for-profit membership organisation for country code Top Level Domain (ccTLD) Registries like .uk. It currently has 52 full members and 9 associate members that between them manage over 80% of all domain names registered within ccTLDs.

8.14 In 2008, CENTR surveyed its members about their practices relating to the release of zone file data. 29 CENTR members responded to the survey and Table 4 below lists those registries that did, at that time, make zone file data available and those that did not.

Zone File data made available (As reported in 2008)	Zone File date NOT made available (As reported in 2008)
	.de Germany *.nl Netherlands* *.eu European Union* *.pl Poland* *.es Spain*
.it Italy *.at Austria* *.cz Czech Republic* *.dk Denmark* *.fi Finland* *.ie Ireland* *.jp Japan* *.nz New Zealand* *.sk Slovakia*	*.be Belgium* *.am Armenia* *.cat Catalonia* *.is Iceland* *.ir Iran* *.il Israel* *.lv Latvia* *.lt Lithuania* *.lu Luxembourg* *.mt Malta* *.mx Mexico* *.no Norway* *.pt Portugal* *.ro Romania* *.se Sweden*

Table 4

- Of 29 the responding registries 9 did make zone file data available while 20 did not.
- 7 members of the current top 20 ccTLD list reported their zone file practices.
- Of those, 6 did not provide access to zone file data, between them representing some 33.7 million ccTLD domain name registrations.
- Only Italy's *.it* did provide access to zone file data. The *.it* register now has around 2.6 million domain names registered.

8.15 The terms of access operated by these members were as follows:

- Of the 9 registries that did provide access to zone file data, only one (*.sk* Slovakia) offered full public access (by publishing the zone file on its website).
- In all other cases zone file access was made available either to a selected client group only, with restrictions on how the data can be used, or both.

8.16 The most common reasons cited by those registries that did not publish zone file data were concerns over data protection issues or other potential abuses of the data such as the sending of spam. Furthermore, 14 registries noted that they had provided this service in the past but had since stopped. The most common reasons for this change were concerns over various forms of abuse of the data, again the potential for its use for spam being frequently cited.

8.17 Plainly, therefore, there is not a unified approach amongst ccTLD registries. But it appears that the following points can be made:

- The majority of ccTLD registries that responded to the 2008 survey do not make zone file data available.
- Fears over potential abuses of the data were reported as a major factor underlying this majority stance.
- Where access to zone file data was offered, it was only done so under certain restrictive terms.

Nominet's current practice

8.18 At present Nominet does not make its full zone file data available. I am told that its reasoning includes the following:

- Nominet considers the *.uk* register and the data contained within it to be important and valuable IP, owned by Nominet.
- Although Nominet acknowledges that public access to the zone file would have the merit of providing extra eyes on the register (and, perhaps, improved public confidence), that must be balanced against the opportunity that public access brings for abuse of the data.
- This might include illicit use of the register to generate spam email lists, and an ability for typo-squatters to abuse access to the register to generate lists of close matches to existing commercial or banking domain names.

8.19 I do not regard the argument that the register is a piece of IP owned by Nominet to be at all an attractive argument in the context of not making public its zone file. However, and more compellingly, Nominet has expressed strong doubts that raw zone file data is the best tool to assist in rights protection and criminal law enforcement. Rather, Nominet takes the view that more filtered and targeted data sets are likely to be more useful, particularly to the police undertaking criminal investigations. In this context, Nominet appears to have in mind a service it currently operates known as the Public Register Search Service (PRSS).

The PRSS Tool

8.20 PRSS is subscription tool offered by Nominet that allows the subscriber to search the *.uk* register for specific strings within domain names, as well as domains that are registered to a particular registrant.

8.21 The scope of searches can be widened using wildcards. Subscribers can store regular searches as favourites, keep a history of their last 1,000 searches for speedy access, and set up alerts for any new registrations containing specified strings.

8.22 As well as being a tool which is apparently widely used for defending intellectual property rights, the PRSS is also employed by law enforcement agencies and is likely useful in the investigation and prosecution of criminal offences. The PRSS is also widely used for academic research and for various governmental functions.

8.23 The PRSS is available to everyone based in the EEA and presently costs £400+ VAT per year. I am told that various laws firms and IP agencies maintain subscriptions. The PRSS is also made available at no charge to public bodies such as the IWF and police agencies on request.

8.24 There are currently 95 active PRSS subscriptions including:

- Advertising Standards Authority
- City of London Police, National Fraud Intelligence Bureau
- Internet Watch Foundation
- Medicines and Healthcare Products Regulatory Agency
- Metropolitan Police
- National Policing Improvement Agency
- National Trading Standards e-Crime Central Intelligence Hub
- Office of Fair Trading
- Scottish Crime and Drug Enforcement Agency
- Serious Organised Crime Agency (Now NCA)

Data release policy

8.25 In addition, Nominet operates a data release policy in accordance with its data protection responsibilities and will release the registration details for individual domain names at the request of relevant law enforcement agencies.

WHOIS policies

8.26 Finally, Nominet requires accurate data regarding domain name registrants and individual domain name records are made public via a WHOIS (a secure domain name search tool) look-up. There are opt-out entitlements for non-trading individuals only and complaints procedures are in place for third parties who believe a *.uk* domain name is either showing incorrect WHOIS data, or has incorrectly opted out of the WHOIS.

Conclusion

8.27 It seems to me there is a strong argument that to permit very broad public access to Nominet's register would help to increase public confidence, in the sense that it would empower individuals, as well as agencies and organisations, to raise any concerns about the appropriateness of particular domain names.

8.28 I have, however, concluded that the counter-arguments, relating to the importance of holding the register in conditions of some security in order to defeat the purposes of those who would seek to abuse access for criminal ends, are more powerful.

8.29 I have reached this conclusion in circumstances where, as I have explained earlier in this report, I do not believe that Nominet should assume a role in scrutinising domain names on taste or offensiveness grounds. This means that the very many complaints on grounds of taste or offensiveness that might be thrown up by broad public access to the register would, in my view, serve no useful purpose, even as the process itself raised the risk of the serious abuse of registry information by criminals.

8.30 At the same time, the ability of law enforcement to gain access to the register at no cost, and Nominet's data release policy, described above, mean that where the issue is not one of taste or offensiveness, but of potential criminality, the PRSS tool guarantees access to the relevant law enforcement agencies so that appropriate scrutiny may take place.

8.31 It is true that zone file access allows the subscriber to assemble an extended list of domain names matching a chosen search string, with perhaps tens of thousands of matches. However, it is worth noting that it was this sort of extremely lengthy list that the IWF concluded was not a useful starting point for any scrutiny, given the inevitability that such a mechanism will produce an overwhelming majority of false positives.

8.32 In contrast, I understand that PRSS limits search returns to a weekly allowance and consequently mandates shorter and more targeted lists. I am told that Nominet is not aware that this limit causes any issues for law enforcement users; indeed a recent check of the active law enforcement and IWF accounts did not identify any that were approaching the limit of allowed searches.

8.33 In addition, PRSS permits the start point in any analysis to be a search for domain names registered under a particular name or close matches to it, which could plainly be a useful exercise. Searches of a zone file do not allow offer this facility, as the file does not include any registrant data.

8.34 Finally, zone file data allows subscribers to start looking at the IP addresses or mail services associated with identified domain names and this may well be a useful investigative tool. However, PRSS provides a parallel facility for IP addresses by allowing the subscriber to identify the IP addresses associated with highlighted domain names and to run new searches that cross-reference highlighted domain names against any identified IP addresses of interest.

8.35 On balance, I have concluded that Nominet's policy of allowing access to its register through the PRSS tool offers a satisfactory degree of transparency and an efficient mechanism to law enforcement, while at the same time maintaining an appropriate degree of security in relation to data, access to which could be of great assistance to spam generators and other criminals. I note that a number of law enforcement agencies do indeed subscribe to this tool, and that Nominet does not charge law enforcement any fee for this service.

9. COMPLAINTS

9.1 As I have indicated, Nominet already runs a Dispute Resolution Service ('DRS') to deal with complaints that .uk sites contain material that infringes copyright or raises disputed trademark issues. Many companies aggressively protect their trademarks and take action against what they regard as abuses or improper exploitation.

9.2 In these circumstances, Nominet maintains a panel of expert assessors to make judgments between competing arguments and the parties are bound by the results, which can lead to no action, suspension or de-registration of the domain name in question. Nominet apparently sees this process as part of its mission to keep .uk a safe space for trade and commerce.

9.3 The question arises as to whether Nominet should create a similar process to deal with complaints that particular domain names appear to signal or to incite crime, or that .uk websites appear to have content that is in some way criminal.

9.4 In my view, there are a number of reasons why such a DRS style process would not be appropriate in the case of complaints of a criminal nature.

9.5 Firstly, in the case of complaints that a website, or even a domain name itself, may be criminal, speed is obviously of the essence. DRS is a careful process impacting on the rights of the parties, and it can take some time to conclude. In this sense it is prima facie ill suited as a response to allegations of crime.

9.6 Secondly, the whole basis of the DRS system is that it is a form of arbitration in which both sides cooperate and agree to be bound by the outcome. That is hardly likely to be the case in the context of criminal allegations.

9.7 Thirdly, allegations of criminal conduct are necessarily the business of state agencies, including the police and prosecutors. It could hardly be appropriate for a private organisation like Nominet to be making determinative judgements in this area, still less for it to be farming those judgments out to an external panel working on commercial terms whose conclusions would then be regarded as determinative.

9.8 Indeed I believe it is precisely the analysis that complaints of alleged criminal conduct are for the state to resolve, rather than for private organisations or individuals, which leads to a clear conclusion that Nominet's role in this area must be highly circumscribed. It seems plain that where it receives an allegation from a member of the public that the content of a .uk website is

criminal, or that a .uk domain name signals or incites serious crime, Nominet can do no more than to examine the material to satisfy itself whether this may indeed be the case. It is, I think, only in these strictly defined circumstances that Nominet should involve itself in any examination of website content.

9.9 If it is clear to Nominet that the website content may well be criminal, or that the .uk domain name may well signal or amount in itself to serious crime, it should refer the matter either to the police, or to the relevant registrar for further action. Of course this further action could, in consultation with the police, amount to suspension or de-registration.

9.10 If it is unclear to Nominet that there is anything problematic in the material brought to its attention, it should do no more than advise the complainant of their freestanding right further to complain to the hosting registrar, or to the police.

9.11 In my view, Nominet lacks both the skills and the remit to undertake determinative assessments of complaints that essentially amount to allegations of crime, and it would be wholly inappropriate to redraft Nominet's role to graft these duties onto its business. They would be inconsistent with its status as a private company, forcing upon Nominet a criminal regulatory role over the Internet for which it is ill equipped.

9.12 I also think it likely that such a development would be inconsistent with public confidence in the .uk space. The most action that Nominet should be obliged to undertake in the case of allegations of crime is to make a judgement about whether material appears to pass a threshold that means it should properly be referred to the police. This is a judgement that is made by citizens day in and day out.

9.13 For the avoidance of doubt, in the case of complaints which appear to turn, not on an analysis as to whether criminal conduct may be in play, but rather on questions of taste and decency, Nominet should make it plain to complainants that, in accordance with Article 10 of the European Convention and given its role and the nature of its remit, it has no power to act.

9.14 In the case of referrals from the police, the situation is obviously different. Here, Nominet should swiftly agree an appropriate course of action in consultation with police. This action could obviously include suspension or de-registration of the domain name in question.